The Canonical Types of Nets of Modular Conics.

BY ALBERT HARRIS WILSON.

INTRODUCTION.

1. In this paper is treated the following problem. Given three ternary quadratic forms,

$$C_i = a_i t_1^2 + 2h_i t_1 t_2 + b_i t_2^2 + 2g_i t_1 t_3 + 2f_i t_2 t_3 + c_i t_3^2, \qquad (i=1, 2, 3), \tag{1}$$

belonging to the $GF(p^n)$; it is proposed to reduce the net of forms

$$R = xC_1 + yC_2 + zC_3 \tag{2}$$

(x, y, z likewise in the $GF(p^n)$), to canonical types by means of linear transformations operated simultaneously on the t_i, on the one hand, and on the x, y, z, on the other. The t_i will be referred to as the variables, and the x, y, z as the parameters; and a transformation of these latter (which replaces any C by a linear combination of the C_i), as a parameter change. By canonical types is to be understood what is usually implied by that term in algebra; namely, types equivalent in the aggregate, under the transformations mentioned, to the nets (2), and which contain the minimum number of arbitrary constants, such constants as do appear being invariants of the net.

The analogous problem for the ordinary complex-number field has been completely solved by Jordan.* In this field the vanishing points of the C_i are curves of the second order, and the discriminant of the net is a cubic curve, the locus of the points (x, y, z) for which the quadratic $R(t_1, t_2, t_3)=0$ is degenerate. The treatment is based upon the invariant theory and the geometric properties of the cubic, and the canonical forms are derived in an elegant manner. They are sixteen in number, classified by the mutual relations of the three curves $C_i=0$ and the form of the discriminant.

In the finite field the analogy of geometry may still be useful. The vanishing points of the quadratics are conics in the Veblen-Bussey finite geometry,†

* C. Jordan, "Réduction d'un réseau de formes quadratiques ou bilineares," *Journal de Mathématiques* (1906), 7.

† Veblen-Bussey, "Finite Projective Geometries," *Transactions of the American Mathematical Society*, Vol. VII, 1906.

and those of the discriminant of the net a cubic curve. Unquestionably the most advantageous method of attacking the problem would be the usual one of a classification based upon the discriminant; but the theory of the cubic curve and its invariants in finite geometry is at present in so undeveloped a state that little progress could be made with it. Under the circumstances it has seemed best to make use of the following purely algebraical method, though aid is at times derived from geometrical intuition, and frequently geometrical nomenclature is employed.

2. *Analysis of the Problem.* The net (2), $R=xC_1+yC_2+zC_3$, regarded as a quadratic in t_1, t_2, t_3, $R=a_{11}t_1^2+2a_{12}t_1t_2+a_{22}t_2^2+2a_{13}t_1t_3+2a_{23}t_2t_3+a_{33}t_3^2$, has for its discriminant

$$D=\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix},$$

a ternary cubic form in x, y and z. The discussion of the net may be separated into parts according to the rank of the determinant D.

In the first place, the case of the identical vanishing of D (for all values of x, y and z) may be excluded, as this would mean that the ternary quadratic $R(t_1, t_2, t_3)$ was reducible to a binary form. Also the case where the quadratics C_i are not linearly independent may be set aside, for then the net degenerates into a family of two forms, or into a single form. The determinant may then be of rank 1, 2 or 3, meaning by this of minimum rank 1, 2 or 3 for any values of x, y, z not all zero; and it is on this basis of division that the problem is discussed in what follows.

D is of rank 1. Values of x, y, z exist (always excluding $x=y=z=0$) for which the first minors of D vanish simultaneously. In this case the net contains a unary form; and conversely, values of x, y, z which make R a unary form will cause all the first minors to vanish.

D is of rank 2. Values of x, y, z exist which will make D vanish, but no values exist which will cause all the first minors to vanish. In this case the net contains a binary form, but no unary form; the converse of this statement is likewise true.

D is of rank 3. No values of x, y, z exist for which D vanishes. The net in this case contains neither a binary nor a unary form. The existence of this net is in itself remarkable and occurs only when the coefficients of R are subjected to narrow conditions.*

*The discriminant cubic is the locus of the points (x, y, z) for which the corresponding conic degenerates into two lines or into a double line. The above classification of the discriminant is then a classification of the nets into those which contain (i), degenerate conics which are double lines; (ii), degenerate

PART I. THE DISCRIMINANT OF THE NET IS OF RANK 1.

3. *Separation of the Cases.* There is by hypothesis a unary form in the net, and we may set $C_1=t_1^2$. Then by a parameter change, subtracting C_1 from C_2 and C_3,

$$C_2=at_2^2+bt_2t_3+ct_3^2+dt_1t_2+et_1t_3, \quad C_3=a't_2^2+b't_2t_3+c't_3^2+d't_1t_2+e't_1t_3.^*$$

One of the following three cases must exist:

(a) No one of the terms t_2^2, t_2t_3, t_3^2 appears either in C_2 or C_3.

(b) One or more of the terms t_2^2, t_2t_3, t_3^2 appears in one form of the net, but not in the others.

(c) The terms t_2^2, t_2t_3, t_3^2 appear in both forms, C_2 and C_3, in such a way that this case is not reducible to (b).

4. *In the first of the hypotheses,* (a), writing the forms C_1, C_2, C_3, in order, to indicate the net, we have t_1^2, $at_1t_2+bt_1t_3$, $a't_1t_2+b't_1t_3$, which is obviously readily reduced in all cases to

$$\text{I.}^\dagger \qquad t_1^2, \quad 2t_1t_2, \quad 2t_1t_3. \tag{4}$$

5. *In the second of the hypotheses,* (b), *of* § 3, the net is

$$t_1^2, \quad at_1t_2+bt_1t_3, \quad f+d't_1t_3+e't_1t_2, \tag{5}$$

where f represents the binary quadratic $a't_2^2+b't_2t_3+c't_3^2$. f may be transformed, without affecting the forms of C_1 or C_2, into one of the following: t_2^2, t_3^2, $t_2^2+t_3^2$, or $t_2^2+vt_3^2$, where v represents a particular not-square.‡ The last two forms are usually treated together and written $t_2^2+mt_3^2$, where $m=1$ or v.

---

conics not double lines; and (iii), no degenerate conics. Imaginary points are not considered in this paper.

The number of nets of conics can be gotten as follows: Let $P_k=\frac{p^{(k+1)n}-1}{p^n-1}$ be the number of points in a linear space, S_k. The linear system of conics are in one-to-one correspondence with the points of an S_5. The number of nets of conics is the number of planes (S_2's) in S_5. A plane is determined by a *proper* triangle. Such a triangle can be chosen in $\frac{P_5(P_5-P_0)(P_5-P_1)}{1\cdot2\cdot3}$ ways in S_5; the first point in P_5 ways, the second point (any point except the first) in P_5-P_0 ways, and the third point (any point except those on the join of the first two) in P_5-P_1 ways. But the same plane is determined by any triangle in it. In a plane there are $\frac{P_2(P_2-P_0)(P_2-P_1)}{1\cdot2\cdot3}$ proper triangles. Hence there are $\frac{P_5(P_5-P_0)(P_5-P_1)}{P_2(P_2-P_0)(P_2-P_1)}$ planes in S_5 or nets of conics in S_2.

*In the processes of reduction the letters representing the coefficients are usually repeated, even though they are in the course of the transformation replaced by combinations of the coefficients; for only the types are sought. Only when special values (such as 0) may arise, which affect the validity of the results, is it necessary to attend to the actual values of the coefficients.

† With these same numerals the nets are listed in a final summary.

‡ Dickson, "Linear Groups," §§ 168, 169. The process of transformation of $at_2^2+bt_2t_3+ct_3^2$ by which the term t_2t_3 is eliminated [*i. e.*, by $t_2=t_2'-bt_3'/(2a)$, $t_1=t_1'$, $t_3=t_3'$] we may call, for brevity, completing the square on the terms $at_2^2+bt_2t_3$.

Let $f=t_2^2$ in (5). Completing the square in C_3 and making an easy parameter change, we have t_1^2, $at_1t_2+bt_1t_3$, $t_2^2+b't_1t_3$. If here $b'=0$, there results by $t_3'=at_2+bt_3$ (as $b\neq 0$) the single net

$$\text{IV.} \qquad t_1^2, \quad t_2^2, \quad 2t_1t_3. \tag{6}$$

If $b'\neq 0$ and $b=0$, by $t_2=b't_2'$, $t_1=b't_1'$,

$$\text{II.} \qquad t_1^2, \quad 2t_1t_2, \quad t_2^2+2t_1t_3 \tag{7}$$

If $b'\neq 0$ and $b\neq 0$, we have, on multiplying the variables t_1 and t_2 by b', t_1^2, $at_1t_2+t_1t_3$, $t_2^2+t_1t_3$; and by the transformation $t_1=t_1'$, $t_2=t_2'+at_1'/2$, $t_3=t_3'-at_2'-a^2t_1'/2$, followed by parameter changes, this net becomes t_1^2, t_2^2, $2t_1t_3$, which is IV.

Let $f=t_2t_3$ in (5). If $b=0$, the second form C_2 becomes t_1t_2; if $b\neq 0$, then, by the transformation $t_1=t_1'$, $t_2=t_3'$, $bt_3=t_2'-at_3'$, C_2 becomes t_1t_2. In any case t_1t_2 may be canceled from C_3, and we have t_1^2, t_1t_2, $t_2t_3+c't_1t_3$. If $c'=0$, directly, or, if $c'\neq 0$, by $t_2=t_2'+c't_1'$, this becomes

$$\text{V.} \qquad t_1^2, \quad 2t_1t_2, \quad 2t_2t_3. \tag{8}$$

Let $f=t_2^2+mt_3^2$ in (5). Completing the square on $t_2^2+e't_1t_2$ and $mt_3^2+d't_1t_3$ in C_3, and making parameter changes, there results t_1^2, $at_1t_2+bt_1t_3$, $t_2^2+mt_3^2$. We may here assume that $a\neq 0$; for if $a=0$, then by interchanging t_2 and t_3 the term t_1t_2 is restored in C_2. Set, then, $a=1$. By the transformation $t_1=t_1'$, $t_2=t_2'-bt_3'$, $t_3=t_3'+bt_2'/m$, provided the determinant $1+b^2/m$ does not vanish, the net becomes

$$\text{VII.} \qquad t_1^2, \quad 2t_1t_2, \quad t_2^2+mt_3^2. \tag{9}$$

If, on the other hand, the determinant $1+b^2/m$ of the transformation just used does vanish, multiply t_3 by $-b$: t_1^2, $t_1t_2+mt_1t_3$, $t_2^2-m^2t_3^2$, which by $t_2=(t_2'+t_3')/2$, $t_3=(t_2'-t_3')/2m$ becomes t_1^2, $2t_1t_2$, $2t_2t_3$, a net already enumerated as V.

6. *In the third of the hypotheses,* (c), *of* § 3, the net is written

$$t_1^2, \quad at_2^2+bt_2t_3+ct_3^2+dt_1t_2+et_1t_3, \quad a't_2^2+b't_2t_3+c't_3^2+d't_1t_2+e't_1t_3.$$

Obviously one square term must be present in C_2 or C_3, and this may, without essential restriction, be taken to be t_2^2 in C_2. If the square be completed on the terms $at_2^2+bt_2t_3$ of C_2, and t_2^2 be canceled from C_3, there results

$$t_1^2, \quad t_2^2+ct_3^2+dt_1t_2+et_1t_3, \quad b't_2t_3+c't_3^2+d't_1t_2+e't_1t_3. \tag{10}$$

If $b'=0$, (10) becomes

$$t_1^2, \quad t_2^2+dt_1t_2+et_1t_3, \quad t_3^2+d't_1t_2+e't_1t_3 \tag{11}$$

(as t_3^2 must be present in C_3 by hypothesis). If $b' \neq 0$ in (10), then, by $b't_2 + c't_3 = t_2'$ afterwards canceling the resulting t_2t_3 from C_2, the net is

$$t_1^2, \quad t_2^2 + ct_3^2 + dt_1t_2 + et_1t_3, \quad t_2t_3 + d't_1t_2 + e't_1t_3. \tag{12}$$

If $c=0$ in (12), by $t_1 = t_1'$, $t_2 = t_2' - dt_1'/2$, $t_3 = t_3' - d't_1'$, the net reduces readily to

$$t_1^2, \quad t_2^2 + et_1t_3, \quad t_2t_3 + e't_1t_3. \tag{13}$$

If in (13) $e=0$,

$$t_1^2, \quad t_2^2, \quad t_2t_3 + e't_1t_3. \tag{14}$$

If in (13) $e \neq 0 = 2$ (say),

$$t_1^2, \quad t_2^2 + 2t_1t_3, \quad t_2t_3 + e't_1t_3. \tag{15}$$

If in (14) $e'=0$, the net is t_1^2, t_2^2, t_2t_3, which is seen to be equivalent to IV by interchanging t_1 and t_2. If in (14) $e' \neq 0 = 1$ (say), there results

$$\text{VI.} \qquad t_1^2, \quad t_2^2, \quad 2(t_2t_3 + t_1t_3). \tag{16}$$

The net (15) for $e' \neq 0 = 1$ (say) is equivalent to the same net for $e'=0$, *i. e.*, t_1^2, $t_2^2 + 2t_1t_3$, $2(t_2t_3 + t_1t_3)$ to $t_1'^2$, $t_2'^2 + 2t_1't_3'$, $2t_2't_3'$, by the transformation $t_1 = -9t_1'$, $t_2 = 3(t_1' + t_2')$, $t_3 = 2t_1' + t_2' - t_3'$, with non-vanishing determinant,

$$\text{IX.} \qquad t_1^2, \quad 2t_2t_3, \quad t_2^2 + 2t_1t_3. \tag{17}$$

In this reduction it is assumed that $p \neq 3$.

If in (12) $c =$ a square (not 0), then, on multiplying t_2 by the square root of c, the form C_2 becomes $t_2^2 + t_3^2 + dt_1t_2 + et_1t_3$. By $C_2' = C_2 + 2C_3$, followed by $t_2 = t_2' + t_3'$, $t_3 = t_2' - t_3'$, and a parameter change, the net (11) is again obtained.

If finally, in (12), c is a not-square, set it equal to a particular not-square v; there remain for further reduction the nets (11) and

$$t_1^2, \quad t_2^2 + vt_3^2 + dt_1t_2 + et_1t_3, \quad t_2t_3 + d't_1t_2 + e't_1t_3. \tag{18}$$

In (11) complete the square on $t_2^2 + dt_1t_2$ in C_2 and on $t_3^2 + e't_1t_3$ in C_3, and get

$$t_1^2, \quad t_2^2 + et_1t_3, \quad t_3^2 + d't_1t_2. \tag{19}$$

If in (19) $e = d' = 0$, we have

$$\text{III.} \qquad t_1^2, \quad t_2^2, \quad t_3^2. \tag{20}$$

If in (19) $e=0$, $d' \neq 0$, or $e \neq 0$, $d'=0$, by obvious changes we have

$$t_1^2, \quad t_2^2, \quad t_3^2 + 2t_1t_2. \tag{21}$$

If in (19) $e \neq 0$, $d' \neq 0$, multiply t_1 by $2/e$ and get

$$t_1^2, \quad t_2^2 + 2t_1t_3, \quad t_3^2 + 3\rho t_1t_2, \tag{22}$$

where ρ is a parameter, arbitrary, except not 0.

In (18) the squares may be completed to eliminate the terms t_1t_2 and t_1t_3 in C_2, giving

$$t_1^2, \quad t_2^2+vt_3^2, \quad t_2t_3+d't_1t_2+e't_1t_3. \tag{23}$$

If in (23) $d'=e'=0$, there results

$$\text{VIII.} \qquad t_1^2, \quad 2t_2t_3, \quad t_2^2+vt_3^2. \tag{24}$$

If in (23) $d'=0$, $e'\neq 0$, or $d'\neq 0$, $e'=0$,

$$\text{X.} \qquad t_1^2, \quad 2(t_1t_3+t_2t_3), \quad t_2^2+vt_3^2. \tag{25}$$

If in (23) $d'\neq 0$, $e'\neq 0$, then, multiplying t_3 by d' and t_2 by e', we have finally

$$\text{XI.} \qquad t_1^2, \quad 2(t_1t_2+t_1t_3+t_2t_3), \quad t_2^2+\alpha t_3^2, \tag{26}$$

where α is an arbitrary parameter not equal to zero.

7. Two of the nets just obtained and not listed by the Roman numerals, namely, (21) and (22), may now be included under the net XI (26).

In the first place, for $\alpha=1$ in (26), by $C_2'=C_1+C_2+C_3$, the net may be written t_1^2, $(t_1+t_2+t_3)^2$, $t_2^2+t_3^2$; and this, by $t_1=t_1'$, $t_2=-t_1'+t_2'-t_3'$, $t_3=t_3'$, reduces to t_1^2, t_2^2, $t_1^2+t_2^2+2t_3^2-2t_1t_2+2t_1t_3-2t_2t_3$. Cancel t_1^2, t_2^2, and eliminate t_1t_3 and t_2t_3 by completing the square, and there results t_1^2, t_2^2, $t_3^2+2t_1t_2$, which is (21).

Again, the net (22) may be included under XI (26) for α = a square = k^2, $\neq 1$. In fact, if h is chosen so that $h^3=\rho\dfrac{1+k}{1-k}$ (which for every ρ is possible unless $p^n=3$), the substitution

$$t_1=-2t_1', \quad t_2=t_1'+\frac{1+k}{2h}t_2'+\frac{1+k}{2h^2}t_3', \quad t_3=t_1'-\frac{1+k}{2hk}t_2'+\frac{1+k}{2h^2k}t_3'$$

will transform t_1^2, $2(t_1t_2+t_1t_3+t_2t_3)$, and $t_2^2+k^2t_3^2$ into members of the net $xt_1^2+y(t_2^2+2t_1t_3)+z(t_3^2+2\rho t_1t_2)$.

8. *Independence of the Nets.* It remains to determine whether the nets just found are independent of each other; that is, incapable of being transformed, one into the other, by linear transformations of the variables or the parameters. Many of the questions of equivalence are answered by an examination of the invariants of the nets. The rank of the determinant shows the independence, as classes, of the three classes of nets which are separately examined in this paper; no net which contains a unary form can be equivalent to a net which contains no unary form. The numerical invariants, the number

of the unary forms and the number of the binary forms, will in many cases serve to distinguish the nets. Further, the form of the discriminant $D(x, y, z)$, which is multiplied in the transformation on the t_i by the square of the determinant of transformation, will aid in answering the question.

9. As an illustration of the method of reckoning these invariants, consider the case of the net XI, $xt_1^2+2y(t_1t_2+t_1t_3+t_2t_3)+z(t_2^2+\alpha t_3^2)$.

$$D=\begin{vmatrix} x & y & y \\ y & z & y \\ y & y & \alpha z \end{vmatrix}=2y^3-(\alpha+1)y^2z-xy^2+\alpha xz^2.$$

For $D=0$, $(y^2-\alpha z^2)x=2y^3-(\alpha+1)y^2z$. In the case $\alpha=1$, the discriminant is factorable, and this case should be treated separately; however, here, by § 7, the net is equivalent to the simpler one t_1^2, t_2^2, $t_3^2+2t_1t_2$, of which it is readily determined that the number of binary forms, $B,=2(p^n-1)^2$, and the number of unary forms, $U,=2(p^n-1)$. Excluding the case $\alpha=1$, distinguish further the cases α = a square = k^2 (not 0), and α = a not-square.

$\alpha=k^2$. If $y=z=0$, the determinant vanishes for x arbitrary, only not 0; *i. e.*, for p^n-1 values. If y and z are arbitrary, only not $y=z=0$, there are $p^{2n}-1$ sets of values; but from these must be deducted the number of sets for which the multiplier of x also vanishes (except $y=z=0$); for these will not cause D to vanish unless $\alpha=1$. These latter sets given by $y=\pm kz$ are $2(p^n-1)$ in number. The total number of vanishing sets is then $p^n-1+p^{2n}-1-2(p^n-1)=p^n(p^n-1)$. To find how many of these are unary forms, consider the first minors of the discriminant: $xz-y^2$, $y(x-y)$, $y(y-z)$, $\alpha xz-y^2$, $y(\alpha z-y)$, αz^2-y^2. As $\alpha\neq 1$, these vanish together only for $y=z=0$; *i. e.*, for p^n-1 sets of values of x, y, and z. Hence, finally, $B=p^n(p^n-1)-(p^n-1)=(p^n-1)^2$, $U=p^n-1$.

α = a not-square. The multiplier of x can not be made to vanish except for $y=z=0$, for which, for x arbitrary (not 0), the discriminant vanishes. Further, as in the case of $\alpha=k^2$. The number of vanishing sets for D is then $p^{2n}+p^n-2$, or $B=(p^n+1)(p^n-1)$, $U=p^n-1$.

10. By an examination of the character of the discriminant and the numerical invariants, all questions of equivalence are answered except the following: IV may be equivalent to VI, and X may be equivalent to XI for $\alpha=v$. (See pp. 208, 209 for table of nets.)

If IV is equivalent to VI, then each of the forms t_1^2, t_2^2, t_1t_2 must go into one of the type $xt_1^2+2y(t_1t_3+t_2t_3)+zt_2^2$ by a transformation $t_1=at_1'$, $t_2=bt_2'$, $t_3=c_1t_1'+c_2t_2'+c_3t_3'$, or else $t_1=at_2'$, $t_2=bt_1'$, $t_3=c_1t_1'+c_2t_2'+c_3t_3'$. By these t_1t_3

becomes $a(c_1t_1^2+c_2t_1t_2+c_3t_1t_3)$ or $a(c_1t_1t_2+c_2t_2^2+c_3t_2t_3)$; but neither of these is of the required type.

11. *Equivalence of the Nets* X *and* XI *for* α = *a not-square* v. If $p^n=4k-1$, *i. e.*, if -1 is a not-square, set $v=-1$. Then the transformation

$$t_1=-2t_1', \quad t_2=2t_1'+t_2'+t_3', \quad t_3=t_2'-t_3'$$

will take each form of X into XI; *i. e.*, t_1^2, $t_1t_3+t_2t_3$, and $t_2^2+t_3^2$ into

$$Xt_1^2+2Y(t_1't_2'+t_1't_3'+t_2't_3')+Z(t_2'^2-t_3'^2).$$

If $p^n=4k+1$ (-1 a square), the equivalence of the two nets is conditional. As an example of discussions of this kind, this case is treated in detail.

The net $xC_1+yC_2+zC_3$ is equivalent to $XC_1'+YC_2'+ZC_3'$ if C_1, C_2, and C_3 are severally capable of being transformed into forms of the type $XC_1'+YC_2'+ZC_3'$. The form t_1^2 must go into the form $at_1'^2$, as there is but one (essential) unary form in each of the nets. Hence the reduction is effected, if at all, by a transformation of the form

$$t_1=at_1', \quad t_2=b_1t_1'+b_2t_2'+b_3t_3', \quad t_3=c_1t_1'+c_2t_2'+c_3t_3', \tag{27}$$

of determinant $a(b_2c_3-b_3c_2)$. By this the three forms of XI must be transformed into forms of the type X. Substituting in the last two forms of XI, and equating coefficients with those of X, we have the two sets of equations:

$$\begin{aligned} 2(ab_1+ac_1+b_1c_1)&=X, & b_1^2+vc_1^2&=X',\\ 2b_2c_2&=Z, & b_2^2+vc_2^2&=Z',\\ 2b_3c_3&=vZ, & b_3^2+vc_3^2&=vZ',\\ a(b_2+c_2)+b_1c_2+b_2c_1&=0, & b_1b_2+vc_1c_2&=0,\\ a(b_3+c_3)+b_1c_3+b_3c_1&=Y, & b_1b_3+vc_1c_3&=Y',\\ b_2c_3+b_3c_2&=Y, & b_2b_3+vc_2c_3&=Y'. \end{aligned}$$

From the second and third of each set Z may be eliminated, and from the fifth and sixth Y, giving,

(A$_1$) $b_3c_3-vb_2c_2=0$, (B$_1$) $vb_2^2-b_3^2+v^2c_2^2-vc_3^2=0$,

(A$_2$) $a(b_2+c_2)+b_1c_2+b_2c_1=0$, (B$_2$) $b_1b_2+vc_1c_2=0$,

(A$_3$) $a(b_3+c_3)+b_3(c_1-c_2)+c_3(b_1-b_2)=0$, (B$_3$) $b_3(b_1-b_2)+vc_3(c_1-c_2)=0$.

It is readily seen that none of the letters can be 0. Setting from (A$_1$): $b_2=lb_3$, $vc_2=c_3/l$, $(l\neq 0)$, there results from (B$_1$) $lb_3=c_3$, or $lb_3=-c_3$. Supposing first $lb_3=c_3$, we have $lb_3=c_3=b_2=lvc_2$; and substituting successively in the remaining equations, (A$_2$), (A$_3$), (B$_2$), (B$_3$), we find all the coefficients expressed in terms of a, as follows:

$$\left.\begin{array}{lll} 2lb_3=-(1+vl)a, & b_2=lb_3, & b_1(1-l^2v)=2lb_3, \\ c_3=lb_3, & vc_2=b_3, & c_1(1-l^2v)=-2l^2b_3, \end{array}\right\} \tag{28}$$

which will effect the transformation in question, provided

$$l^3v^2+3l^2v+3lv+1=0. \tag{29}$$

As $p^n=4k+1$, $v\neq-1$, $1+l^2v\neq0$, $1-l^2v\neq0$, the last expression is, to within a non-vanishing factor, the discriminant of the transformation.

Similarly, from the second hypothesis, $lb_3=-c_3$, there are derived:

$$\left.\begin{array}{lll} 2lb_3=(1-vl)a, & b_2=lb_3, & (1-l^2v)b_1=2lb_3, \\ c_3=-lb_3, & vc_2=-b_3, & (1-l^2v)c_1=2l^2b_3, \end{array}\right\} \tag{30}$$

provided

$$l^3v^2-3l^2v+3lv-1=0. \tag{31}$$

If either of the equations (29), (31) is reducible, the other is also. Now the conditions for the irreducibility of equations in Galois fields has been fully discussed by Professor Dickson,* and, in particular, the following result obtained: The necessary and sufficient conditions that the cubic $x^3+bx+c=0$ be irreducible, are

(1) $\quad -4b^3-27c^2=$ a square $\neq0$, say $81m^2$, (32)

(2) $\quad \frac{1}{2}(-c+m\sqrt{-3})=$ a not-cube for field $[GF(p^n), \sqrt{-3}]$. (33)

Multiply the roots of (29) by v and write $l-1$ for l, and it takes the following form: $l^3+3(v-1)l-2(v-1)=0$. The conditions for irreducibility are now

$$\left.\begin{array}{ll} (1) & -108(v-1)^3-108(v-1)^2=81m^2, \\ (2) & \frac{1}{2}[2(v-1)+m\sqrt{-3}]=\text{ a not-cube in } [GF(p^n), \sqrt{-3}]. \end{array}\right\} \tag{34}$$

The first condition requires that 3 be a not-square (as $p^n=4k+1$); hence $p^n=12k+5$. Take $v=-3$, then $m=8$, and the second condition requires that $4(-1+\sqrt{-3})$, or equally, that $\frac{1}{2}(-1+\sqrt{-3})$, shall be a not-cube. This latter number is ω, a cube root of 1. If now $\omega=r^3$, then $\omega^3=r^9=1$, where $r^3\neq1$, r in $GF(p^{2n})$. Hence 9 is a factor of $p^{2n}-1$; but as $p^n-1\equiv1$ (mod. 3), it follows that $p^n+1\equiv0$ (mod. 9). From $p^n=12k+5$ follows then $k\equiv1$ (mod. 3).

---

* *Bulletin of the American Mathematical Society,* October, 1906.

Hence the equation $l^3v^2+3l^2v+3lv+1=0$ is reducible, and the net X equivalent to XI, except for $p^n=36k+17$; and it results from equations (A_1), ..., (B_3) that in this latter case the nets are not equivalent.

PART II. THE DISCRIMINANT OF THE NET IS OF RANK 2.

12. *Separation of the Cases.* There is by hypothesis a binary form in the net, but no unary form; hence we may set

$$\left.\begin{aligned} &C_1=t_1^2+mt_2^2,\ (m=1 \text{ or } v, \text{ a particular not-square}),\\ &C_2=at_1^2+bt_1t_2+ct_1t_3+dt_2t_3+et_3^2,\\ &C_3=a't_1^2+b't_1t_2+c't_1t_3+d't_2t_3+e't_3^2,\end{aligned}\right\} \tag{35}$$

canceling t_2^2 from C_2 and C_3. Under any circumstances we may take $e=0$. If also $e'=0$, cancel t_2t_3 from C_2 and write the net:

$$t_1^2+mt_2^2,\quad at_1^2+bt_1t_2+ct_1t_3,\quad a't_1^2+b't_1t_2+c't_1t_3+d't_2t_3. \tag{36}$$

If $e'\neq0$ in (35) the square may be completed to eliminate from C_3 the terms t_1t_3 and t_2t_3, and the net be written:

$$t_1^2+mt_2^2,\quad at_1^2+bt_1t_2+ct_1t_3+dt_2t_3,\quad a't_1^2+b't_1t_2+t_3^2. \tag{37}$$

13. In the net (36) distinguish the cases $c=0$, $c\neq0$. If $c=0$, then $b\neq0$; otherwise a unary is present. Setting $b=1$, and canceling t_1t_2 from C_3:

$$t_1^2+mt_2^2,\quad at_1^2+t_1t_2,\quad a't_1^2+c't_1t_3+d't_2t_3. \tag{38}$$

If $c\neq0$, then, by $t_3'=at_1+bt_2+ct_3$, and canceling t_1t_3 from C_3':

$$t_1^2+mt_2^2,\quad t_1t_3,\quad a't_1^2+b't_1t_2+d't_2t_3. \tag{39}$$

The net (38), by $t_2'=at_1+t_2$ and parameter change, becomes

$$t_1^2+mt_2^2,\quad t_1t_2,\quad a't_1^2+c't_1t_3+d't_2t_3. \tag{40}$$

Since c' and d' are not both 0 in (40), say $c'\neq0=1$, set $t_3'=a't_1+t_3$, and the net becomes $t_1^2+mt_2^2$, t_1t_2, $t_1t_3+d't_2t_3$; or, if $d'\neq0$, $t_1^2+ft_2^2$, t_1t_2, $t_1t_3+t_2t_3$, on multiplying t_1 by d'. Write $f=r^2$ or $f=r^2v$ according as f is a square or a not-square; the net is brought, by the substitution $t_1=t_1'r+t_2'$, $t_2=-\frac{r}{f}t_1'-t_2'$, $t_3=t_3'$, into the form

$$\text{XII.}\qquad t_1^2+vt_2^2,\quad 2t_1t_2,\quad 2t_1t_3. \tag{41}$$

The transformation is inadmissible if $f=1$; but in this case, by adding $2C_2$ to C_1, a unary results. If $d'=0$ in (40), net XII is reached directly.

In the net (39) $d'=0$ readily reduces to (41); set $d'=1$. For $a'=b'=0$ there results

$$\text{XIII.}\qquad t_1^2+mt_2^2,\quad 2t_1t_3,\quad 2t_2t_3. \tag{42}$$

If $b'\neq 0$, multiplying t_3 by b':

$$\text{XIV} \qquad t_1^2+mt_2^2, \quad 2t_1t_3, \quad \beta t_1^2+2t_1t_2+2t_2t_3, \qquad (\beta \text{ arbitrary}). \tag{43}$$

If $a'\neq 0$, $b'=0$, the net is $t_1^2+mt_2^2$, t_1t_3, $at_1^2+t_2t_3$. By $C_3-aC_1=C_3'$, followed by $t_3=-amt_3'$: $t_1^2+mt_2^2$, t_1t_3, $t_2(t_2+t_3)$. By $t_3'=t_2+t_3$: $t_1^2+mt_2^2$, $t_1t_2+t_1t_3$, t_2t_3. Interchanging t_1 and t_2 and multiplying C_1, there results: $t_1^2+mt_2^2$, t_1t_3, $t_1t_2+t_2t_3$, which is XIV for $\beta=0$.

14. If in net (37) $c=d=0$, then $b\neq 0$, and setting $t_2'=at_1+bt_2$, we have, on canceling t_1t_2 from the resulting C_2 and C_3, $t_1^2+ft_2^2$, t_1t_2, $a't_1^2+t_3^2$. As above, f may be reduced to v, and multiplying t_3 by $\sqrt{a'}$ if a' is a square, and by b if $a'=vb^2$, the net becomes

$$\text{XV.} \qquad t_1^2+vt_2^2, \quad t_1t_2, \quad t_1^2+mt_3^2. \tag{44}$$

If c and d are not both 0 in the net (37), we may take $c\neq 0$ and set $c=1$. Then, by the transformation

$$t_1'=t_1+dt_2, \quad t_2'=-\frac{d}{m}t_1+t_2, \quad t_3'=t_3, \tag{45}$$

if the determinant $\dfrac{d^2}{m}+1\neq 0$, the net takes the form

$$t_1^2+mt_2^2, \quad at_1^2+bt_1t_2+t_1t_3, \quad a't_1^2+b't_1t_2+t_3^2.$$

By $t_3'=at_1+t_3$, followed by a parameter change, we have

$$t_1^2+mt_2^2, \quad bt_1t_2+t_1t_3, \quad a't_1^2+b't_1t_2+t_3^2. \tag{46}$$

To reduce this, certain values of the coefficients must be excepted. For $b=b'=0$, the net is easily seen to reduce to XV. For $b=0$, $b'\neq 0$, we may write $t_3=b''t_3'$, where $b'=m'b''^2$, ($m'=1$ or v), and we obtain

$$t_1^2+mt_2^2, \quad t_1t_3, \quad a't_1^2+2m't_1t_2+t_3^2;$$

and finally, setting $m't_1=t_1'$, the net becomes

$$\text{XVI.} \qquad t_1^2+\lambda t_2^2, \quad 2t_1t_3, \quad \gamma t_1^2+2t_1t_2+t_3^2, \tag{47}$$
$$(\lambda=1,\ v,\ v^2, \text{ or } v^3;\ \gamma \text{ arbitrary}).$$

In (46), for $b\neq 0$ set $t_3=bt_3'$ and cancel t_1t_2 from C_3: $t_1^2+mt_2^2$, $t_1t_3+t_1t_2$, $a't_1^2+b't_1t_3+t_3^2$. In this complete the square to eliminate t_1t_3 from C_3, and obtain

$$\text{XVII.} \qquad t_1^2+mt_2^2, \quad \delta t_1^2+2t_1t_2+2t_1t_3, \quad \varepsilon t_1^2+t_3^2, \tag{48}$$
$$(\delta,\ \varepsilon \text{ arbitrary, except } \varepsilon\neq 0).$$

15. There remains to be considered, from the net (37), the case where the determinant of the transformation (46), $\frac{d^2}{m}+1$, vanishes. For this case $t_1=\frac{1}{2}(t'_1+t'_2)$, $t'_2=\frac{1}{2d}(t'_1-t'_2)$, and easy parameter changes, give t_1t_2, $at_1^2+bt_2^2+t_1t_3$, $a't_1^2+b't_2^2+t_3^2$; and this, by $t'_3=at_1+t_3$, becomes

$$t_1t_2, \quad bt_2^2+t_1t_3, \quad a't_1^2+b't_2^2+t_3^2. \tag{49}$$

If in (49) $b\neq 0$, we obtain, on multiplying t_1 and t_3 by suitably chosen constants,

$$t_1t_2, \quad t_2^2+t_1t_3, \quad at_1^2+\lambda t_2^2+t_3^2, \qquad (\lambda=0,\ 1,\ \text{or}\ v).$$

If $\lambda=0$, permute t_2 and t_3, and multiply these letters to reduce the net to

$$t_1^2+mt_2^2, \quad t_1t_3, \quad t_3^2+m't_1t_2,$$

which is XVI for $\gamma=0$. If $\lambda\neq 0$, by $C'_3=C_3-\lambda C_2$, and then completing the square on $t_3^2-\lambda t_1t_3$ in C'_3, we have $t_3^2+at_1^2$, t_1t_2, $\frac{\lambda}{2}t_1^2+t_1t_3+t_2^2$. Permute here t_3 and t_2, multiply these letters by suitably chosen constants, and get

$$t_1^2+mt_2^2, \quad t_1t_3, \quad \rho t_1^2+2m't_1t_2+t_3^2,$$

which is XVI.

If in (49) $b=0$, by obvious changes the net becomes

$$t_1t_2, \quad t_1t_3, \quad \lambda t_1^2+\lambda' t_2^2+t_3^2, \qquad (\lambda,\ \lambda'=0,\ 1,\ \text{or}\ v). \tag{50}$$

$\lambda=\lambda'=0$ is excluded; otherwise C_3 is a unary form. $\lambda=0$ gives XIII. $\lambda'=0$ gives XII. $\lambda=\lambda'=1$ or v, gives, by $C'_3=2C_1+C_3$, t_1t_2, t_1t_3, $(t_1+t_2)^2+mt_3^2$; this, by $t'_2=t_1+t_2$, permuting t_1 and t_3 in the result, and eliminating t_2t_3, becomes

$$t_1^2+mt_2^2, \quad t_1t_2+t_1t_3, \quad mt_1^2+t_3^2,$$

which is included in XVII. $\lambda=1$, $\lambda'=v$ is equivalent to $t_1^2+t_2^2+vt_3^2$, t_1t_2, t_1t_3. By $C'_1=2C_2+C_1$, $t'_2=t_1+t_2$, and an interchange of t_1 and t_3 in the result:

$$t_1^2+vt_2^2, \quad t_1t_3, \quad t_3^2+t_2t_3,$$

which is XVI for $\gamma=0$. $\lambda=v$, $\lambda'=1$, gives

$$vt_1^2+t_2^2+t_3^2, \quad t_1t_2, \quad t_1t_3;$$

this net is equivalent to XVII for $\delta=0$, $\varepsilon=m=1$ by the transformation

$$t_1=b_3t'_2-b_2t'_3, \quad t_2=t'_1+b_2t'_2+b_3t'_3, \quad t_3=t'_1-b_2t'_2-b_3t'_3,$$

where $v(b_2^2+b_3^2)=1$, applied to XVII.

16. *Independence of the Nets of Part* II. To use the discriminant to its full value in separating the nets, we examine for what cases the discriminants

of XIV, XVI, and XVII are factorable. To illustrate the method, the details are given for the case of XIV.

$D=2yz^2+mxy^2-z^2(x+\beta z)$. Set $y=rx+sz$ in this and simplify. D becomes

$$mr^2x^3+2mrsx^2z+(2r-1+ms^2)xz^2+(2s-\beta)z^3.$$

In order that this vanish identically, $r=0$, $s^2=\frac{1}{m}$, $\beta=2s$; then $m=1$, $s=\pm 1$, $\beta=\pm 2$; and for this value of β, $y\pm z$ is a factor of $D=(y\pm z)(2z^2+xy\mp xz)$. There is evidently no factor free of y.

Examining similarly the discriminant of XVI, we find that it is never factorable.

The discriminant of XVII, $D=mx^2z-mxy^2+m\varepsilon xz^2+m\delta xyz-y^2z$, is found by the above method to have a factor in case $\delta=0$, $\varepsilon=\frac{1}{m}$; in fact, for these values $D=(xz-y^2)(mx+z)$. The number of binary forms in this case is $2p^n(p^n-1)$ or $2(p^n+1)(p^n-1)$, according as $-m$ is a square or a not-square. This number is the same as that for XV, but the two nets may be shown to be distinct by the method of § 11.

The number of binary forms is calculated as in § 9. For nets XVI and XVII this number appears to be so difficult to calculate, that it seems best to take up the question of their independence from another point of view. There are, of course, no unary forms in these nets.

It is seen at once that XII, XIII, XIV, and XV are independent of each other even for the factorable case of the discriminant of XIV. Moreover, XII, XIII, and XIV are independent of XVI and XVII. This leaves for examination the relations between the nets XIV, XVI, and XVII.

17. *Relations between* XIV *and* XVI. To examine this we proceed to attempt the transformation of the discriminant of one into that of the other multiplied by a square. To this end a device is used which depends on the following lemma:*

LEMMA. *If a ternary cubic form $f(x, y, z)$ becomes $F(X, Y, Z)$ under the linear transformation*

$$x=AX+BY+CZ,\quad y=A_1X+B_1Y+C_1Z,\quad z=A_2X+B_2Y+C_2Z, \tag{51}$$

and u denotes $f(A, A_1, A_2)$, then

$$\frac{1}{2}\frac{\partial^2 F}{\partial X^2}=x\frac{\partial u}{\partial A}+y\frac{\partial u}{\partial A_1}+z\frac{\partial u}{\partial A_2}. \tag{52}$$

---

* This Lemma and its application are due to Professor Dickson.

Proof: If we set

$$u_B=B\frac{\partial u}{\partial A}+B_1\frac{\partial u}{\partial A_1}+B_2\frac{\partial u}{\partial A_2},\quad u_C=C\frac{\partial u}{\partial A}+C_1\frac{\partial u}{\partial A_1}+C_2\frac{\partial u}{\partial A_2},$$

we have

$$F=uX^3+u_BX^2Y+u_CX^2Z+\ldots,$$

$$\frac{1}{2}\frac{\partial^2 F}{\partial X^2}=3uX+u_BY+u_CZ=(AX+BY+CZ)\frac{\partial u}{\partial A}$$
$$+(A_1X+B_1Y+C_1Z)\frac{\partial u}{\partial A_1}+(A_2X+B_2Y+C_2Z)\frac{\partial u}{\partial A_2},$$

since by Euler's theorem of homogeneous functions

$$3u=A\frac{\partial u}{\partial A}+A_1\frac{\partial u}{\partial A_1}+A_2\frac{\partial u}{\partial A_2}.\quad \text{Q. E. D.}$$

Replace, in the discriminant of XVI, γ by $2\sigma/\lambda$; it then becomes

$$f=-z^3+2\sigma xz^2+\lambda x^2z-\lambda xy^2,\qquad (\lambda\neq 0). \tag{53}$$

Suppose that under the transformation (51) f becomes

$$F=d^2(2YZ^2+mXY^2-XZ^2-\beta Z^3), \tag{54}$$

which differs from the discriminant of XIV only by a square factor. Since F is linear in X, (52) must vanish, so that $\frac{\partial u}{\partial A}=\frac{\partial u}{\partial A_1}=\frac{\partial u}{\partial A_2}=0$; we have then $2\sigma A_2^2+2\lambda AA_2-\lambda A_1^2=0$, $AA_1=0$, $-3A_2^2+4\sigma AA_2^2+\lambda A^2=0$. Let the modulus p^n exceed 3. In view of the determinant of (51), A, A_1, and A_2 can not all be 0; hence, taking $A_1=0, A_2\neq 0, A=-\sigma\lambda^{-1}A_2$, whence $\lambda=-\sigma^2, A_1=0, A=\sigma^{-1}A_2\neq 0$. In view of the last relation, $z_1=z-\sigma x$ is free of X. Hence we set

$$x=x_1,\quad y=y_1,\quad z=z_1+\sigma x_1. \tag{55}$$

Then $f=-z_1^3-\sigma x_1z_1^2+\sigma^2x_1y_1^2$, and

$$x_1=AX+BY+CZ,\quad y_1=bY+cZ,\quad z_1=rY+sZ. \tag{56}$$

Now $\frac{\partial f}{\partial X}=\frac{\partial f}{\partial x_1}\frac{\partial x_1}{\partial X}+\ldots=A(\sigma^2y_1^2-\sigma z_1^2), \frac{\partial F}{\partial X}=d^2(mY^2-Z^2)$. Since these binary forms must be equivalent, the ratio of their discriminants must be a square. Thus σ/m must be a square; but as in XIV m may be multiplied by any square, we may set $m=\sigma$. By the theory of binary forms the only transformations replacing $\sigma A(\sigma y_1^2-z_1^2)$ by $d^2(\sigma Y^2-Z^2)$ are

$$y_1=bY+cZ,\quad z_1=\pm\sigma cY\pm bZ, \tag{57}$$

where $\sigma A(b^2-\sigma c^2)=d^2$.

Set in (56) $r=\pm\sigma c$, $s=\pm b$, and noting the relation (57), transform f and equate to F. On reducing the conditions we find that the transformation

will replace f by F if, and only if,

$$d^2B=\pm A\sigma^2c^3,\quad d^2C=\pm 3A\sigma bc^2,\quad d^2\beta=\pm b^3\pm 3\sigma bc^2,\quad d^2=\mp\frac{1}{2}\sigma c(3b^2+\sigma c^2). \tag{58}$$

The simplest values of b and c which make the final expression a square, are $b=0$, $c=-2$, with the upper signs holding. For this choice (57) and (58) give $d^2=4\sigma^2$, $A=-1$, $B=2$, $C=0$, $\beta=0$. Hence by (55) and (56)

$$x=-X+2Y,\quad y=-2Z,\quad z=-\sigma X. \tag{59}$$

Now the net XIV, with $m=\sigma$, $\beta=0$, is $X(t_1^2-\sigma t_2^2)+2Yt_1t_3+2Z(t_1t_2+t_2t_3)$, while the net XVI, with $\lambda=-\sigma^2$ and γ replaced by $2\sigma/\lambda$ (as above), is

$$x(t_1'^2-\sigma^2t_2'^2)+2yt_1't_2'+z(-2\sigma^{-1}t_1'^2+2t_1't_2'+t_3'^2).$$

If these are equivalent under the correspondence (59), the coefficients of X, $2Y$, and $2Z$ must be equivalent:

$$t_1^2-\sigma t_2^2=t_1'^2-2\sigma t_1't_2'+\sigma^2t_2'^2-\sigma t_3'^2,\quad t_1t_3=t_1'^2-\sigma^2t_2'^2,\quad t_1t_2+t_2t_3=-2t_1't_3'.$$

Hence, apart from constant factors, $t_1=t_1'-\sigma t_2'$, $t_2=-t_3'$, $t_3=t_1'+\sigma t_2'$. Thus a net of XVI is equivalent to some net of XIV if, and only if, $\lambda\gamma^2=-4$ in XVI.

18. *Relation between* XIV *and* XVII. By examining these nets in exactly the same way as XIV and XVI were examined in § 17, we arrive at the result: A net of XVII is equivalent to some net of XIV if, and only if, in XVII $m=-1$, and $4\varepsilon+(\delta\pm 2)^2=0$.*

19. *Relation between* XVI *and* XVII. The invariants, S and T, of a cubic form furnish the absolute invariant, S^3/T^2. For brevity write $\sigma=\lambda\gamma^2$ in XVI and $Q=\delta\varepsilon-4\delta-4\varepsilon$ in XVII. The value of this invariant for the two discriminants is as follows:

$$D_{\text{XVI}}:\quad \frac{S^3}{T^2}=-\frac{(3+\sigma)^3}{16(9+2\sigma)^2},$$

$$D_{\text{XVII}}:\quad \frac{S^3}{T^2}=-\frac{(Q^2-48\delta\varepsilon)^3}{64Q^2(Q^2-72\delta\varepsilon)^2}$$

(first multiplying t_2 and t_3 in XVII by δ). A necessary condition for the equivalence of the nets is the equivalence of these two invariants. If we put $a=\sigma+4$, $b=Q^2-64\delta\varepsilon$, $c=-16\delta\varepsilon$, and then $a'=b/c$, this condition becomes

$$\frac{(a'-1)^3}{(a'-4)(a'+1/2)}=\frac{(a-1)^3}{(a-4)(a+1/2)},$$

* The cases of equivalence between the nets XIV, XVI, and XVII just found receive a new interpretation when the discriminants of the nets are regarded as cubic curves in finite geometry. The discriminant of XIV put equal to 0 is a cubic with a double point; that of XVI has a double point if $\lambda\gamma^2+4=0$, and that of XVII if $m=-1$, $4\varepsilon+(\delta\pm 2)^2=0$. The conditions derived by use of the lemma, namely,

$$\frac{\partial u}{\partial A}=\frac{\partial u}{\partial A_1}=\frac{\partial u}{\partial A_2}=0,$$

are obviously equivalent to the conditions for a double point of the cubic.

where $a=0$, $a'=0$ are, respectively, the conditions for a double point of the cubic curves $D_{\text{XVI}}=0$, $D_{\text{XVII}}=0$.

If we attack the problem of direct transformation of the net XVI into XVII, it is possible to express the conditions to which the parameters are subjected for equivalence, but these conditions are in an exceedingly long and awkward form.

PART III. THE DISCRIMINANT OF THE NET IS OF RANK 3.

20. That nets exist which contain neither a unary nor a binary form may be proved from the results of a paper by Professor Dickson.* Setting out from the theorem that any field which contains an irreducible cubic $f(r)=0$ has for the norm of the function $x+ry+r^2z$ a ternary cubic form which vanishes in the field only for $x=y=z=0$, the conditions are determined that the general cubic shall have this property. We shall apply these conditions as they are derived from a simplified form of the cubic, when, namely, by an obvious transformation, the terms in x^2y, x^2z, and xyz have been made to disappear. Then, for the cubic

$$a'x^3+d'xy^2+e'xz^2+g'y^3+h'y^2z+k'yz^2+l'z^3, \tag{60}$$

the *necessary and sufficient conditions that this vanish in the field only for* $x=y=z=0$ *are:*

$$\left.\begin{array}{l} \text{(A) } a'q^3+d'q+g'=0 \text{ shall be reducible in the } GF(p^n), \\ \text{(B) } a'd'h' \neq 0, \\ \text{(C) } d'k'+3e'g'=0, \\ \text{(D) } e'h'+3d'l'=0, \\ \text{(E) } 4d'^2e'+3a'h'^2-9a'g'k'=0. \end{array}\right\} \tag{61}$$

21. *Reduction of the Net.* The family of two ternary quadratics which contains no binary form may be readily reduced to $C_1=t_1^2-t_2t_3$, $C_2=2t_1t_2+t_2^2+at_3^2$, where a has a fixed value not 0. Adjoin now a third form which by hypothesis can not be reduced to a binary form; by parameter change it may be written $C_3=2bt_1t_3+ct_1^2+t_2^2+dt_3^2$, the coefficient of t_2^2 being put equal to 1, since it can not vanish, as C_3 is not a binary.

22. The discriminant of the net

$$x(t_1^2-2t_2t_3)+y(2t_1t_2+t_2^2+at_3^2)+z(2bt_1t_3+ct_1^2+t_2^2+dt_3^2) \tag{62}$$

is

$$D=\begin{vmatrix} x+cz & y & bz \\ y & y+z & -x \\ bz & -x & ay+dz \end{vmatrix} =x^3+cx^2z-axy^2-dxz^2-(a+d-2b)xyz+ay^3$$
$$+(d-ac)y^2z-(ac+cd-b^2)yz^2+(b^2-cd)z^3. \tag{63}$$

In order to apply the conditions (61) cited above on this cubic, it must be so

* "Triple Algebras and Cubic Forms," *Bulletin of the American Mathematical Society*, January, 1908.

transformed that the terms in x^2z and xyz shall disappear without introducing the term x^2y. Write in D $x=x'-cz'/3$, $y=y'$, $z=z'$, and the term x^2z will disappear. The terms in $x'y'^2$ and $x'y'z'$ will become $-ax'y'^2-(a+d-2b)x'y'z'$; then by $x'=x''$, $y'=y''-(a+d-2b)z''/2a$, $z'=z''$, the term in $x'y'z'$ will disappear. The result of the two transformations is the cubic (60), where now

$$\left.\begin{aligned}
a'&=1,\\
d'&=-a,\\
e'&=(3a^2-12ab-4ac^2-6ad+12b^2-12bd+3d^2)/12a,\\
g'&=a,\\
h'&=(-9a-4ac+18b-3d)/6,\\
k'&=(3a^2-12ab+4ab^2-8abc+2ad+12b^2-4bd-d^2)/4a,\\
l'&=(-27a^3+36a^3c+162a^2b+108a^2b^2+16a^2c^3\\
&\qquad+72a^2bc-27a^2d-72a^2cd-324ab^2+216ab^3-288ab^2c\\
&\qquad+72abcd+108abd-108ab^2d+36acd^2+27ad^2\\
&\qquad+216b^3-108b^2d-54bd^2+27d^3)/216a^2.
\end{aligned}\right\}\quad(64)$$

For these values of $a', \ldots, l'$, the conditions (61) become

$$\left.\begin{aligned}
&\text{(A)}\ \ q^3-aq+a=0 \text{ shall be irreducible,}\\
&\text{(B)}\ \ a(9a+4ac-18b+3d)\neq 0,\\
&\text{(C)}\ \ ab^2-2abc+ac^2+2ad+2bd-d^2=0,\\
&\text{(D)}\ \ 4a^3c+9a^2b^2+2a^2bc-3a^2c^2-8a^2cd-6a^2d\\
&\qquad\quad+18ab^3-20ab^2c-9ab^2d+6abc^2+2abcd\\
&\qquad\quad+6abd-ac^2d+4acd^2+3ad^2+12b^2d-12bd^2+3d^3=0,\\
&\text{(E)}\ \ a^3-4a^2b+6a^2c-2a^2d-5ab^2+6abc-4abd+2acd+ad^2+3d^2=0.
\end{aligned}\right\}\quad(65)$$

23. *Reduction of the Conditions* (65). With regard to condition (A), it is easily seen that an irreducible cubic exists for every field. In fact, when $q^3-aq+a=0$ is reducible, then a $(\neq 0)$ may be expressed as $q^3/(q-1)$, and conversely. But there can not be more than p^n-2 such values (since $q\neq 0, 1$); that is, there is at least one value of a which will make the equation irreducible. (See § 25.)

The key to the simplification of the conditions (65) (C), (D), and (E) lies in (C), which may be written:

$$a(b-c)^2=d(d-2a-2b). \tag{66}$$

Suppose, first, $d=0$. Then from (C), since $a\neq 0$, $b=c$, while (D) and (E) alike reduce to $(a+b)^2=0$. That is

$$b=c=-a, \tag{67}$$

while (B) becomes $4a-27\neq 0$. Here, then, in the case $d=0$, there is a single net whose fundamental forms are

$$t_1^2-2t_2t_3, \quad 2t_1t_2+t_2^2+at_3^2, \quad -2at_1t_3-at_1^2+t_2^2, \tag{68}$$

where a is so chosen that $a\neq 0$, $4a-27\neq 0$, and $q^3-aq+a=0$ is irreducible.

Suppose, next, that $d\neq 0$ in (66). From (66) we may set $b-c=df$, whence

$$\left.\begin{aligned} 2b&=d-adf^2-2a, \\ 2c&=d-adf^2-2df-2a. \end{aligned}\right\} \tag{69}$$

For these values of b and c, (D) and (E) become, respectively,

$$\left.\begin{aligned} a^3f^4+12a^2f^3+2a^2f^2-20af+a+12=0, \\ (2a^3f^3-64a^2f^3-20a^2f^2+112af-5a-64)d-a^2(a^2f^3-af+1)=0; \end{aligned}\right\} \tag{70}$$

or, putting

$$af=z, \tag{71}$$

equations (70) take the form

$$\left.\begin{aligned} z^4+12z^3+2az^2-20az+a^2+12a=0, \\ [(2a-64)z^3-20az^2+112az-5a^2-64a]d-a^2(z^3-az+a)=0. \end{aligned}\right\} \tag{72}$$

24. *Discussion of the Quartic* (72). The quartic

$$z^4+12z^3+2az^2-20az+a^2+12a=0$$

has one, and but one, root in the field. In the paper to which reference has been made in § 11, the conditions for irreducibility of the cubic and quartic are explicitly set forth; in particular, it is there proved that a quartic has one, and but one, root in the field if the resolvent cubic is irreducible. Now the resolvent cubic of the quartic in question is

$$y^3-2ay^2+(-4a^2-288a)y+8a^3-448a^2-(12)^3a=0.$$

In order to apply the conditions for the irreducibility of the cubic, the term in y^2 is first eliminated. Set $y=2x$, and divide by 8 to simplify:

$$x^3-ax^2+(-a^2-72a)x+a^3-56a^2-216a=0.$$

In this set $x=X+a/3$:

$$X^3-(72a+4a^3/3)X+16a^3/27-80a^2-216a=0. \tag{73}$$

The discriminant of this cubic is

$$a^24^3(64a^3-9^2\cdot 16a^2-6\cdot 27\cdot 54a-(27)^3=4^3a^2(4a-27)^3. \tag{74}$$

Now the cubic $x^3-ax+a=0$ is known to be irreducible, and the two conditions for this (see § 11, end) are

$$\left.\begin{aligned} 4a-27&=\text{ a square }=81e^2 \text{ (say)}, \\ \frac{1}{2}(-a+ae\sqrt{-3})&=\text{ a not-cube in } [GF(p^n),\ \sqrt{-3}]. \end{aligned}\right\} \tag{75}$$

Applying the conditions of irreducibility to (73):

$$\left.\begin{array}{r}4^3a^2(4a-27)^3=\text{ a square }=81(8\cdot 81\cdot ae^3)^2,\\ \frac{1}{2}(-b+8\cdot 81\cdot ae^3\cdot\sqrt{-3})=\text{ a not-cube in }[GF(p^n),\sqrt{-3}],\end{array}\right\}\quad(76)$$

where $b=16a^3/27-80a^2-216a$. Using the second of (75), the second of (76) is equivalent to the statement

$$(-b+8\cdot 81\cdot ae^3\cdot\sqrt{-3})/(-a+ae\cdot\sqrt{-3})=\text{ a cube in }[GF(p^n),\sqrt{-3}].$$

Multiplying numerator and denominator by $-a-ae\sqrt{-3}$ and reducing, this fraction becomes $36a-36\cdot 27+\sqrt{-3}\cdot e(4a-28\cdot 27)$; but this is equal to

$$9\cdot 81e^2-(27)^2+\sqrt{-3}\cdot e[81e^2-(27)^2]=3^6(-1-e\sqrt{-3}/3)^3.$$

It is thus seen that the cubic resolvent is irreducible, and hence the quartic (72) has one, and but one, root in the field.

25. *Determination of the Coefficients from the Remaining Conditions.* Set the single root of the quartic (72) in the cubic (72), and the value of d is uniquely determined, provided the coefficient of d in that equation does not vanish. By hypothesis the term free of d, $(z^3-az+a)a^2$, is different from 0. Having determined d, (71) and (69) give f, b, and c uniquely. Condition (B), (65), becomes, as $a\neq 0$, $a^2(27-4a)+d(7z^2-4az+2a^2-6a)\neq 0$, so that in this case also, $4a-27\neq 0$.

Denote the coefficient of d in the cubic of (72) by C, and the quartic of (72) by Q, and examine

$$Q=z^4+12z^3+2az^2-20az+a^2+12a=0,$$
$$C=(2a-64)z^3-20az^2+112az-5a^2-64a=0,$$

to determine whether or not they have a common root. The first step in the highest-common-factor process leads to the identity

$$2(a-32)^2Q-[(a-32)z+(22a-384)]C=a^2T,$$

where

$$T=(4a+72)z^2-35az+2a(a+3).$$

If Q and C have a common factor, then C and T will have this same factor, and conversely. We seek, then, the eliminant of C and T which will vanish for a common root. By Sylvester's method of elimination this invariant has the following determinant form:

$$\begin{vmatrix} 4a+72 & -35a & 2a(a+3) & 0 & 0\\ 0 & 4a+72 & -35a & 2a(a+3) & 0\\ 0 & 0 & 4a+72 & 35a & 2a(a+3)\\ 2a-64 & -20a & 112a & -5a^2-64a & 0\\ 0 & 2a-64 & -20a & 112a & -5a^2-64a \end{vmatrix}.$$

From the last two columns a may be removed as a factor. It is then easy to see that the highest power of a that can occur is the sixth.

To complete the proof, we shall show that except for certain low values of p^n, a may be so chosen that the discriminant does not vanish. The choice of a was such as to make the cubic $q^3-aq+a=0$ irreducible.

26. *For how many values of a is the cubic $q^3-aq+a=0$ irreducible?* If this equation be reducible, $a=q^3/(q-1)$, q a mark of the $GF(p^n)$ not 0 nor 1. Let r be also one of these marks and determine for what values of q in terms of r, other than $q=r$, the following equation is satisfied:

$$q^3/(q-1)=r^3/(r-1).$$

Removing the factor $q-r$, we have $q^2(r-1)+q(r^2-r)=r^2$, or if $r\neq 1$, $(2q+r)^2=r^2(r+3)/(r-1)$. Hence, if $(r+3)/(r-1)$ is a square, not 0, there are exactly three of the marks which give the same a; namely, the value of r making $(r+3)/(r-1)$ a square, and the two values of q from the quadratic just written. If $(r+3)/(r-1)$ is a not-square, each corresponding r gives a distinct a. Finally, if $(r+3)/(r-1)=0$, that is $r=-3$, $q=3/2$, and there is an a different from all the rest; that is to say, the two marks -3, $3/2$ always give an a, and it is different from every other a. Let now r run through the sequence of all the marks of the field except 0, 1, 3/2, and -3. Then $(r+3)/(r-1)$ will take all these values except -3, 1, 9, and 0. If, first, -3 is a square, there are $(p^n-1)/2$ not-squares among the values of $(r+3)/(r-1)$, and hence as many a's. There are $(p^n-1)/2-3=(p^n-7)/2$ squares, and therefore $(p^n-7)/6$ a's, and in addition the a that results from the two values $3/2$, -3, of r; in all, $2(p^n-1)/3$ values of a which make the cubic reducible. If -3 is a not-square, there are $(p^n-3)/2$ not-squares $(r+3)/(r-1)$, and hence as many a's; $(p^n-5)/2$ squares, and hence $(p^n-5)/6$ a's, and the additional a; in all, $2(p^n-2)/3$ values of a for which the cubic will be reducible.

The cubic $q^3-aq+a=0$ will be irreducible for $(p^n=1)/3$ or for $(p^n-2)/3+1$ values according as -3 is a square or a not-square in the field. This number will exceed 6, and hence the discriminant in § 24 be not zero if p^n is greater than 19.

27. It thus appears that there are always two nets in which no binary forms occur: one for $d=0$,

$$\text{XVIII.}\qquad t_1^2-2t_2t_3,\quad 2t_1t_2+t_2^2+at_3^2,\quad -2at_1t_3-at_1^2+t_2^2\,; \tag{77}$$

and one for which $d\neq 0$,

$$\text{XIX.}\qquad t_1^2-2t_2t_3,\quad 2t_1t_2+t_2^2+at_3^2,\quad 2bt_1t_2+ct_1^2+t_2^2+dt_3^2, \tag{78}$$

where a is fixed, not 0 nor 27/4, $q^3-aq+a=0$ irreducible, and b, c, and d determined uniquely by (69), ..., (72).

28. *The case of* $p^n=3k+1$ deserves especial notice on account of the simple form which the conditions take. In fact, for this field the family of two forms may be reduced to $x(t_1^2-2t_2t_3)+y(2ut_1t_2-t_3^2)$, u being a particular not-cube.* The net of three forms may readily be put in the form:

$$t_1^2-2t_2t_3, \quad 2ut_1t_2+t_3^2, \quad 2rt_1t_3+st_1^2+t_2^2+tt_3^2. \tag{79}$$

The discriminant of this net is

$$x^3+sx^2z-txz^2+(2ur-1)xyz+u^2y^3+u^2ty^2z-syz^2+(r^2-st)z^3.$$

The conditions that this cubic vanish only for $x=y=z=0$, are best expressed directly as obtained on page 163 of the *Bulletin of the American Mathematical Society*, January, 1908, by Professor Dickson:

$$\left.\begin{array}{ll}(\mathrm{A}') & 2utr+2t+s^2=0,\\ (\mathrm{B}') & 2s+u^2s^2t-4u^2r^2s-2urs+3u^2t^2=0,\\ (\mathrm{C}') & 3s^2+8u^2st^2-5u^2r^2t-4urt+t=0,\\ (\mathrm{D}') & 2ur-1\neq 0.\end{array}\right\} \tag{80}$$

By $(\mathrm{C}')-3(\mathrm{A}')$:

$$t(8u^2st-5u^2r^2-10ur-5)=0. \tag{81}$$

Hence, either $t=0$ or $8u^2st-5u^2r^2-10ur-5=0$. If $t=0$, by (A′) $s=0$; this brings us to an alternative condition (page 164 of above citation),

$$27u^2r^2=-(2ur-1)^3;$$

or, setting $ur=w$:

$$8w^3+15w^2+6w-1=(w+1)^2(8w-1)=0, \tag{82}$$

whence $r=-1/u$ or $r=1/8u$. Eliminating s^2 from (B′) and (A′):

$$2s-4u^2r^2s-2urs+u^2t^2-2u^3t^2r=(1-2ur)(2s+2urs+u^2t^2)=0.$$

Therefore, $2s(1+ur)=-u^2t^2$. Squaring this and eliminating s^2 by (A′), $-8(1+ur)^3t=u^4t^4$; and if $t\neq 0$, $[-2(1+ur)/ut]^3=u$, which is impossible. Hence $t=0$, and we have the nets:

$$\left.\begin{array}{lll}t_1^2-2t_2t_3, & t_3^2+2ut_1t_2, & t_2^2-(2/u)\cdot t_1t_3,\\ t_1^2-2t_2t_3, & t_3^2+2ut_1t_2, & t_2^2+(1/4u)\cdot t_1t_3.\end{array}\right\} \tag{83}$$

In each case the condition (D′) requires that the modulus be not 3.

29. *Summary.* The net $R=xC_1+yC_2+zC_3$ of ternary forms

$$C_i=a_it_1^2+2h_it_1t_2+b_it_2^2+2g_it_1t_3+2f_it_2t_3+c_it_3^2,$$

in the $GF(p^n)$, has been reduced to nineteen canonical types: namely, I, ..., XI, which contain a unary form; XII, ..., XVII, which contain a binary form but no unary; XVIII, XIX, which contain neither unary nor binary forms. All questions of inter-relations between these types have been considered and answered, except with respect to the two cases, nets XVI and XVII, and nets XVIII and XIX.

---

*Dickson, *Quarterly Journal,* § 8, No. 156, 1908. The examination of the net for $p^n=3k+1$ was also made by Professor Dickson.

TABLE

	C_1	C_2	C_3
I	t_1^2	$2t_1t_2$	$2t_1t_3$
II	t_1^2	$2t_1t_2$	$t_2^2+2t_1t_3$
III	t_1^2	t_2^2	t_3^2
IV	t_1^2	t_2^2	$2t_1t_3$
V	t_1^2	$2t_1t_2$	$2t_2t_3$
VI	t_1^2	t_2^2	$2(t_1t_3+t_2t_3)$
VII	t_1^2	$2t_1t_2$	$t_2^2+mt_3^2$
VIII	t_1^2	$2t_2t_3$	$t_2^2+vt_3^2$
IX	t_1^2	$2t_2t_3$	$t_2^2+2t_1t_3$
X	t_1^2	$2(t_1t_3+t_2t_3)$	$t_2^2+vt_3^2$
XI	t_1^2	$2(t_1t_2+t_1t_3+t_2t_3)$	$t_2^2+\alpha t_3^2$
XII	$t_1^2+vt_2^2$	$2t_1t_2$	$2t_1t_3$
XIII	$t_1^2-mt_2^2$	$2t_1t_3$	$2t_2t_3$
XIV	$t_1^2-mt_2^2$	$2t_1t_3$	$\beta t_1^2+2t_1t_2+2t_2t_3$
XV	$t_1^2+vt_2^2$	$2t_1t_2$	$t_1^2+mt_3^2$
XVI	$t_1^2+\lambda t_2^2$	$2t_1t_3$	$\gamma t_1^2+2t_1t_2+t_3^2$
XVII	$t_1^2+mt_2^2$	$\delta t_1^2+2t_1t_2+2t_1t_3$	$\varepsilon t_1^2+t_3^2$
XVIII	$t_1^2-2t_2t_3$	$2t_1t_2+t_2^2+at_3^2$	$-2at_1t_3-at_1^2+t_2^2$
XIX	$t_1^2-2t_2t_3$	$2t_1t_2+t_2^2+at_3^2$	$2bt_1t+ct_1^2+t_2^2+dt_3^2$

OF NETS.

D	B	U
0	$p^n(p^n+1)(p^n-1)$	p^n-1
z^3	$p^n(p^n-1)$	p^n-1
xyz	$3(p^n-1)^2$	$3(p^n-1)$
yz^2	$(2p^n-1)(p^n-1)$	$2(p^n-1)$
xz^2	$2p^n(p^n-1)$	p^n-1
$z^2(y-x)$	$(2p^n-1)(p^n-1)$	$2(p^n-1)$
$mz(xz-y^2)$	$2p^n(p^n-1)$	p^n-1
$x(vz^2-y^2)$	$(p^n+1)(p^n-1)$	p^n-1
z^3-xy^2	$p^n(p^n-1)$	p^n-1
$x(vz^2-y^2)-y^2z$	$(p^n+1)(p^n-1)$	p^n-1
$2y^3-(\alpha+1)y^2z-xy^2+\alpha xz^2$	for $\alpha=1$ $2(p^n-1)^2$ for $\alpha=\sigma^2\neq1$ $(p^n-1)^2$ for $\alpha=v$ $(p^n+1)(p^n-1)$	$2(p^n-1)$ p^n-1 p^n-1
vxz^2	$(2p^n+1)(p^n-1)$	0
$x(my^2-z^2)$	for $m=1$ $3p^n(p^n-1)$ for $m=v$ $(p^n+2)(p^n-1)$	0
$2yz^2+mxy^2-z^2(x+\beta z)$	for $m=1$, $\beta^2=4$ $2p^n(p^n-1)$ for $m=1$, $\beta^2\neq4$ $p^n(p^n-1)$ for $m=v$ $(p^n+2)(p^n-1)$	0
$mz(vx^2-vxy-y^2)$	$2(p^n+1)(p^n-1)$	0
$-z^3+\lambda\gamma xz^2+\lambda x^2z-\lambda xy^2$	?	0
$m\varepsilon xz^2+z(mx^2+m\delta xy-y^2)-mxy^2$	?	0
. . . .	0	0
. . . .	0	0

Remarks. In the above table:

$m=1$ or v, a particular not-square.

$\lambda=1$, v, v^2, or v^3.

α, β, γ, δ, ε are arbitrary parameters, except:

(i) α, ε are not 0;

(ii) net XVI is equivalent to XIV if $\lambda\gamma^2+4=0$;

(iii) net XVII is equivalent to XIV if $m=-1$, $4\varepsilon+(\delta\pm 2)^2=0$.

a, in nets XVIII and XIX, is fixed, not 0 nor $27/4$, and $q^3-aq+a=0$ is irreducible.

b, c, and d, in XIX, are determined uniquely by (69), ..., (72).

For convenience in tabulating the number of binary forms, B, in XIII and XIV, we write in these nets $-m$ for m.